CONTENTS

Introduction to Windows Operating System

- **PowerShell**

  PowerShell consists of two parts: a command-line shell and a scripting language. It started out as a framework to automate administrative tasks in Windows. PowerShell has grown into a cross-platform tool that's used for many kinds of tasks.

  - **Get-Location** – Get the current directory
  - **Set-Location** – Get the current directory
  - **Move-item** – Move a file to a new location
  - **Copy-item** – Copy a file to a new location
  - **Rename** – item Rename an existing file
  - **New-item** – Create a new file

Introduction to Linux Operating System

- Kali Linux is developed, funded and maintained by Offensive Security. It is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools that are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

- All the programs packaged with the operating system have been evaluated for suitability and effectiveness. They include Metasploit for network penetration testing, Nmap for port and vulnerability scanning, Wireshark for monitoring network traffic, and Aircrack-ng for testing the security of wireless networks to name a few.

- The goal of this module is to provide a baseline and prepare users of all skill levels for the upcoming modules.

Introduction to Linux Operating System

Linux file system

- /bin – basic programs (ls, cd, cat, etc.)
- /sbin – system programs (fdisk, mkfs, sysctl, etc)
- /etc – configuration files
- /tmp – temporary files (typically deleted on boot)
- /usr/bin – applications (apt, ncat, nmap, etc.)
- /usr/share – application support and data files
- Man: Man pages contain not only information about user commands, but also documentation regarding system administration commands, programming interfaces, and more.

INSTALLING KALI LINUX VM

User: kali

Password: kali

System Navigation and File Management

1. cp- The cp command is used for copying files or directories from one place to the other. It is good for making copies of files and folders. **Example:**
$ cp file.txt /home/kali/backup/

2. mv- The mv command moves one or more files or directories to another location or changes the name of one or more files or directories.
Example:
$ mv file.txt /home/kali/Documents/

3. pwd- The pwd command is short for 'print working directory'. It is utilized to indicate the absolute location of the directory that the user is currently in. That is when the user wishes to know their present location on the file structure, more so if they are in areas that are characterized by multiple sub-directories.
Example:
$ pwd
/home/kali

4. ls- 'ls' command is what you will use when you want to see the contents of a directory. Its normal usage would be to list files in the working directory and the sub-directories within it, and the sub-directories in turn. To enhance the output, it may also be invoked with -l for a long listing or -a if one wishes to view the hidden files.
Example:
$ ls -la

System Navigation and File Management

5. cd- The cd command means 'change directory', and performs the function of moving between directories.
Example:
$ cd /var/log
$ pwd
/var/log

6. mkdir- The mkdir command is used to create a new folder. **Example:**
$ mkdir new_folder

7. rmdir- The rmdir command is used to remove the empty directory. This is useful on folders that do not contain anything but empty folders, if there are any files or subdirectories in it, they should be emptied before rmdir is executed. To force the removal of a directory, you can use rm -r instead.
Example:
$ rmdir old_folder

8. ping- To check the network connectivity between your computer and a distant host, use the ping command. It waits for a response after sending several ICMP echo requests. The round-trip time for each packet will be displayed if the target host can be reached.
Example:
$ ping google.com

System Navigation and File Management

9. rm- rm stands for remove. This command deletes files and folders from our system. The command uses the -r option for deleting non-empty folders as well the -f option for forceful deletion without prompting.
Example:
$ rm file1.txt

10. ifconfig- The 'ifconfig' is a command that helps in the configuration and management of projects. The command is used to provide interfaces about the current settings on the machine. This includes IP, MAC, subnet mask, and whether the interface is active or not.
Example:
$ ifconfig

11. ps- The 'ps' command assists with displaying the command points or the active processes that are currently performed by your system. The command is normally helpful on its own, however, it can be combined with other options for better sorting and filtering.
Example:
$ ps aux

12. chmod- The 'chmod' command is a command that we can use to change the access control of a file or folder. It may deal with file access such as reading, writing and executing, in which instances we would be setting group, owner, or other.
Example:
$ chmod +x script.sh

Basic Kali Linux Tools

https://www.kali.org/tools/

Intro to Practice Environments

- Bwapp (http://www.itsecgames.com/)
- WebGoat (https://github.com/WebGoat/WebGoat)
- Multillidae (https://github.com/webpwnized/mutillidae)
- DVWA (https://github.com/digininja/DVWA)
- Acunetix (http://www.vulnweb.com/)
- TestVulhub (http://testphp.vulnweb.com/)